602450

RELIABILITY ASSESSMENT OF RECONFIGURABLE FLIGHT CONTROL SYSTEMS USING SURE AND ASSIST [1]

N. EVA WU

DEPARTMENT OF ELECTRICAL ENGINEERING
BINGHAMTON UNIVERSITY
BINGHAMTON, NEW YORK 13902-6000, USA
TEL:(607)777-4375
FAX:(607)777-4464
EMAIL:EVAWU@BINGHAMTON.EDU; N.E.WU@LARC.NASA.GOV

[1]Support by the NASA under Cooperative Agreement NCC-1-336, and by the ASEE Summer Faculty Fellowship is acknowledged.
Thanks to Ricky Butler and Allan White for their time and insightful suggestions.

- OBJECTIVES

○ DEVELOP RELIABILITY ASSESSMENT TOOLS

*SOPHISTICATED SYSTEM CONFIGURATION

*MULTIPLE SOURCES OF UNCERTAINTY

○EVALUATE THE APPLICABILITY OF SURE[4] AND ASSIST[2]

***SURE**: SEMI-MARKOV UNRELIABLITY RANGE EVALUATOR

—APPLICABLE TO A LARGE CLASS OF SEMI-MARKOV MODELS

—EFFICIENT AND ACCURATE

—AVAILABLE FOR VMS/UNIX/MS-WINDOWS OS'

***ASSIST**: ABSTRACT SEMI-MARKOV SPECIFICATION INTERFACE TO THE SURE TOOL

—MODEL GENERATION TOOL FOR DIRECT INTERFACE WITH **SURE**

—POWERFUL AID TO MODELING COMPLEX SEMI-MARKOV PROCESSES

—AVAILABLE FOR VMS/UNIX/MS-DOS OS'

*JUSTIFICATION FOR FURTHER COMPUTATION SIMPLIFICATIONS

—ON-LINE DECISIONS

—UTILITY

• SOME BACKGROUND

∘ MARKOV PROCESS[7]:

$\{X(t) \mid t \in (0,\infty)\}$ IS A MARKOV PROCESS IF $\forall\, t_0 < t_1 \cdots < t_n < t$, THE CONDITIONAL DISTRIBUTION OF $X(t)$ FOR GIVEN VALUES OF $X(t_0), \cdots, X(t_n)$ DEPENDS ONLY ON $X(t_n)$

$$P(X(t) \leq x \mid X(t_n) = x_n, \cdots, X(t_0) = x_0) = P(X(t) \leq x \mid X(t_n) = x_n)$$

∗ HOMOGENEOUS MARKOV PROCESS:

$$P(X(t) \leq x \mid X(t_n) = x_n) = P(X(t - t_n) \leq x \mid X(0) = x_n)$$

—WHITE'S INTERPRETATION:

CONSTANT RATE

INDEPENDENT COMPETING EVENTS

INDEPENDENT SEQUENTIAL EVENTS

$\Rightarrow$

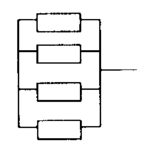
$F(t)$ (TIME A PROCESS SPENDS IN A STATE) IS EXPONENTIAL

$$P(T \leq t) = F(t) = 1 - e^{-F'(0)t}$$

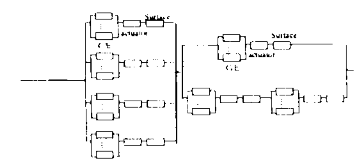
∗ SEMI-MARKOV PROCESS: A MARKOV PROCESS WHOSE DISTRIBUTION IS NOT EXPONENTIAL

• EXAMPLE: AFTI/F-16 FAULT TOLERANT FCS[10]

Functional dependency of subsystems in the FTFCS



Standard



Less standard

∘ A PARALLEL-TO-SERIES INTERCONNECTION OF 5 BLOCKS

∗ FLIGHT CRITICAL PROCESSORS

—POWER SUPPLIES, DIGITAL PROCESSORS

∗ I/O CONTROL MODULE

∗ PILOT COMMAND SENSOR

∗ AIRCRAFT STATE SENSOR

∗ EFFECTOR

—ACTUATORS, SURFACES, INTERFACE UNITS

- SOME PROPERTIES OF THE RELIABILITY MODEL

∘ BUILDING BLOCKS: SUBSYSTEMS (NO SPARES, NO REPAIRS)

∘ REDUNDANCY TYPE: HARDWARE AND FUNCTIONAL

∘ FAILURE: CONTROL PERFORMANCE DEPENDENT

— SUBSYSTEM FAILURE

LACK OF REDUNDANT CONTROL AUTHORITY

∘ FAILURE DETECTION: RESIDUE BASED

RESIDUALS ARE NOISY

—RECONFIGURATION DECISIONS INVOLVE RISKS

∘ MISSION TIME t_m: SHORT

∘ HOLDING TIME DISTRIBUTION $F(t)$: DIFFICULT TO DETERMINE

—NO BASIS FOR ASSUMING EXPONENTIAL

—POSSIBLE TO BOUND BY EXPONENTIAL DISTRIBUTIONS

$$1 - e^{-\lambda_l t} \leq F(t) \leq 1 - e^{-\lambda_u t}, \quad t \leq t_m$$

∘ WHAT TO EXPECT?

—RIGHT ORDERS OF MAGNITUDE

- PROPERTIES (CONT'D) PECULIAR TO FUNCTIONAL REDUNDANCY

∘ SYSTEM ARCHITECTURE: MORE COMPLEX IN GENERAL

* LESS SYMMETRY $\Rightarrow$ HARDER TO OBTAIN A RELIABILITY MODEL

∘ DEATH STATE: DICTATED BY RELIABILITY REQUIREMENTS

* INOPERATIVE WITH MAJORITY

* OPERATIVE WITHOUT MAJORITY

* NO.1 CAUSE OF DEATH $\Rightarrow$ UNSUCCESSFUL RECONFIGURATION

—FALSE ALARM

—MISS DETECTION

—FALSE IDENTIFICATION

—FALSE RECONFIGURATION

* EXHAUSTION OF FUNCTIONAL REDUNDANCY

∘ COVERAGE $C(t)$: NECESSARY

* HIGHLY SCENARIO DEPENDENT;

* VERY DIFFICULT TO ESTIMATE;

* HIGHLY TIME DEPENDENT;

* HARD TIME LIMIT (t_{max} < DEPARTURE TIME)

$$C(t) \approx C(t_{max})$$

- AN EXAMPLE OF CALCULATED COVERAGE

○ SCENARIO —75% LOSS OF CANARD EFFECTIVENESS

○ DATA

—MODEL OF THE AIRCRAFT

MEASURED ANGLE OF ATTACK AND PITCH ANGLE

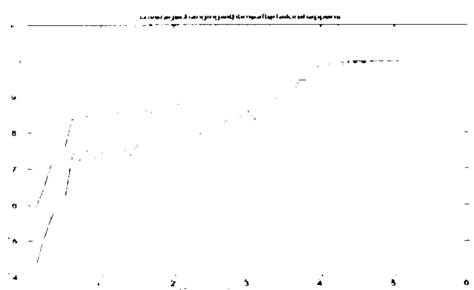
○ FACTORS AFFECTING THE VALUE OF COVERAGE

—PERFORMANCE OF CONTROL, DIAGNOSTIC, DECISION MODULES

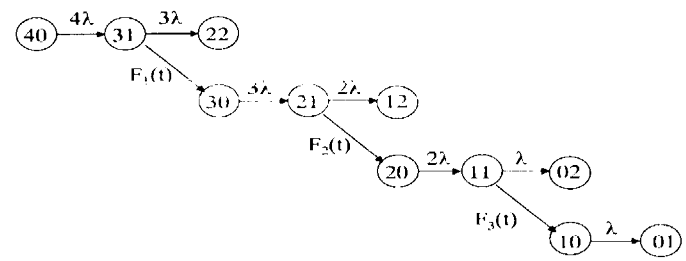
○ RESULTS

—A LUCKY SITUATION OF ACHIEVING 0.9999 AFTER 4.2 SECONDS

—AT T=0.5S, LOWER BOUND OF COVERAGE IS ONLY 0.75

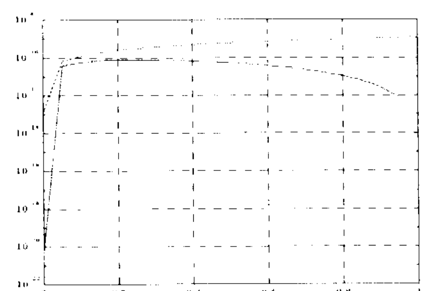


- RELIABILITY ANALYSIS OF THE PROCESSOR BLOCK



Semi-Markov process:
Degradable 4-plex with full reconfiguration

○ BLOCK FAILURE PROBABILITY BOUNDS



$\lambda = 10^{-5}$

$\mu \in [10^{-4}, 10^{0}]$

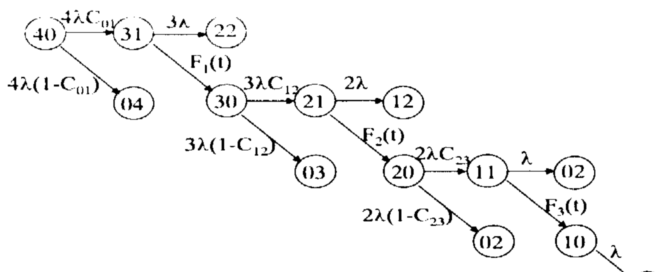
$\sigma = 10^{-2}$

$C_{01} = C_{12} = C_{23} = 1$

$t_m = 1$

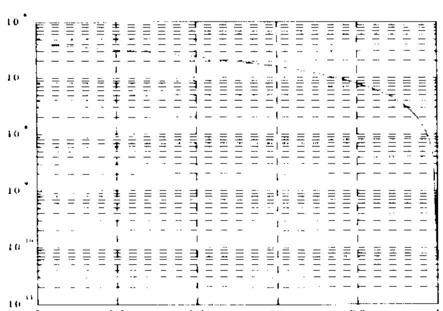
- RELIABILITY ANALYSIS OF THE PROCESSOR BLOCK

  RECONFIGURATION IS NOT COMPLETE



Semi-Markov process:
Degradable 4-plex with incomplete reconfiguration

- BLOCK FAILURE PROBABILITY BOUNDS



$\lambda = 10^{-5}$

$\mu = 10^{-1}$

$\sigma = 10^{-2}$

$C_{01} \in [0.99, 1.0]$

$C_{12} \in [0.95, 1.0]$

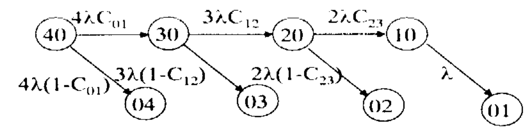
$C_{23} \in [0.90, 1.0]$

$t_m = 1$

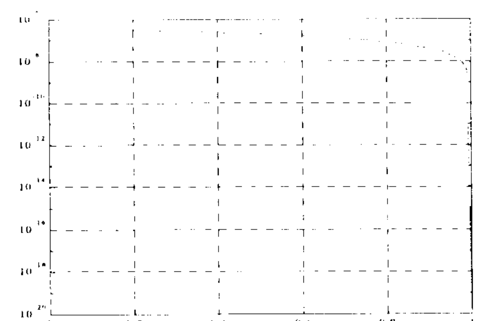
- SURE RELIABILITY ANALYSIS OF THE PROCESSOR BLOCK

  —INSTANTANEOUS REMOVAL OF A FAULTY SUBSYSTEM

Markov process:
Degradable 4-plex with incomplete reconfiguration



- BLOCK FAILURE PROBABILITY BOUNDS



$\lambda = 10^{-5}$

$\mu = 0.0$

$C_{01} \in [0.99, 1.0]$

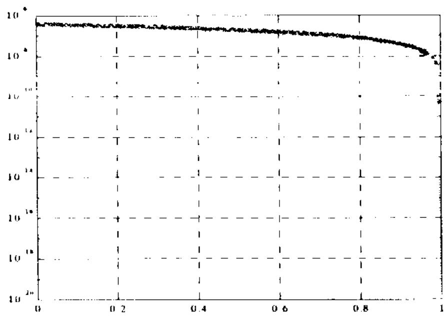
$C_{12} \in [0.95, 1.0]$

$C_{23} \in [0.90, 1.0]$

$t_m = 1$

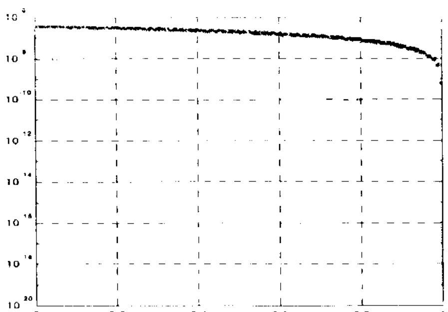
- EFFECTS OF NEGLECTING REMOVAL TIMES

◦ BLOCK FAILURE PROBABILITY BOUNDS



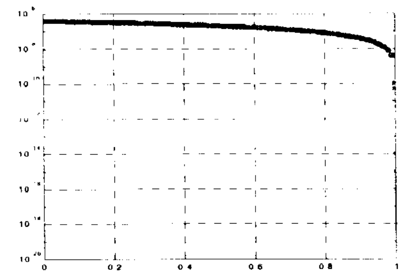
$$\lambda = 10^{-5}$$
$$\mu = 10^{-1}$$
$$C_{01} \in [0.99, 1.0]$$
$$C_{12} \in [0.95, 1.0]$$
$$C_{23} \in [0.90, 1.0]$$
$$t_m = 1$$

◦ BLOCK FAILURE PROBABILITY



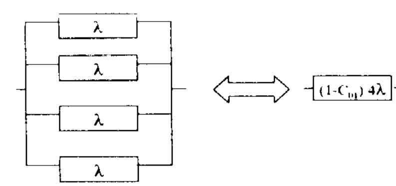
$$\lambda = 10^{-5}$$
$$\mu = 10^{4}$$
$$C_{01} \in [0.99, 1.0]$$
$$C_{12} \in [0.95, 1.0]$$
$$C_{23} \in [0.90, 1.0]$$
$$t_m = 1$$

- FURTHER SIMPLIFICATION OF THE PROCESSOR MODEL



$$p_f \approx (1 - C_{01})4\lambda t_m$$

◦ A SYSTEM WITH AN EQUIVALENT FIRST ORDER EFFECT



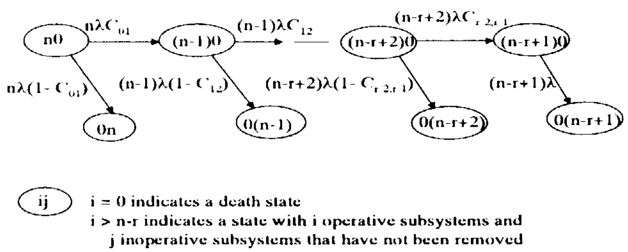
◦ VALID IF RELATIVE TO THE FAILURE PROCESS

- REMOVAL OF FAULTY SUBSYSTEMS IS FAST

MISSION TIME IS SHORT

- JUSTIFICATION OF 2ND APPROXIMATION

◦ AN $r+1$–STATE MARKOV PROCESS



◦ FAILURE OF AN n-SUBSYSTEM BLOCK

— r OR MORE FAILED SUBSYSTEMS, OR

—INCCORECT RECONFIGURATION DECISION

◦ SOME NOTATIONS

—λ: FAILURE RATE OF A SUBSYSTEM

—t_m: MISSION TIME

—$p_{ij}(t)$: TRANSITION PROBABILITY

—C_{ij}: COVERAGE OF A TRANSITION

- COMBINATORY APPROACH

$$P(t) \equiv \begin{bmatrix} p_{00}(t) & p_{01}(t) & p_{02}(t) & \cdots & p_{0r}(t) \\ 0 & p_{11}(t) & p_{12}(t) & \cdots & p_{1r}(t) \\ 0 & 0 & p_{22}(t) & \cdots & p_{2r}(t) \\ \vdots & & & & \vdots \\ 0 & \cdots & & 0 & p_{rr}(t) \end{bmatrix}$$

$$\begin{aligned} p_{ij}(t) &= \binom{n-i}{j-i} q^{j-i}(t)(1-q(t))^{n-i} C_{ij}, && i \le j < r \\ p_{ij}(t) &= 0, && i > j \\ p_{ir}(t) &= 1 - \Sigma_{j=i}^{r-1} p_{ij}(t), && 0 \le i \le r-1 \\ p_{rr}(t) &= 1 \end{aligned}$$

where

$$q(t) = (1 - e^{-\lambda t})$$

IS THE SUBSYSTEM FAILURE PROBABILITY

◦ TRANSITION RATE MATRIX $Q \equiv \dot{P}(0)$

• AN ALTERNATIVE WHEN Q IS KNOWN

$$\dot{P}(t) = P(t)Q(t)$$

WHERE

$P_{(r+1)\times(r+1)}$ IS THE P.T.M.

$Q_{(r+1)\times(r+1)}$ IS THE T.R.M.

$$P_f = [P(t)]_{(1,r+1)}, \quad t \leq t_m$$

○ COMPOSITE FAILURE PROBABILITY

OF m CASCADED BLOCKS

$$1 - \prod_{i=1}^{m} \{1 - [P_i(t)]_{(1,r+1)}\}$$

$$Q = \begin{bmatrix} -n\lambda & C_{01}n\lambda & 0 & \cdots & 0 & [1-C_{01}]n\lambda \\ 0 & -(n-1)\lambda & C_{12}(n-1)\lambda & 0 & \cdots & [1-C_{12}](n-1)\lambda \\ \vdots & 0 & \ddots & & & \vdots \\ 0 & \cdots & 0 & \cdots & -(n-r+1)\lambda & (n-r+1)\lambda \\ 0 & \cdots & & & 0 & 0 \end{bmatrix}$$

○ Q INDEPENDENT OF t

$\Longrightarrow$ HOMOGENEOUS MARKOV PROCESS

$$\begin{aligned} P(t) &= e^{Qt} \\ &= P^N(\frac{t}{N}) \\ &\approx (I + Q\frac{t}{N})^N, \quad \text{EULER APPROXIMATION} \\ &\approx (I + Qt), \quad \text{TAYLOR EXPANSION} \end{aligned}$$

$$\begin{aligned} P_f &= [P(t_m)]_{(1,r+1)} \\ &\approx [Q]_{(1,r+1)} t_m \\ &= [1 - C_{01}]n\lambda t_m \end{aligned}$$

• APPROXIMATION ERROR

$$\begin{aligned} P_f(t) &= [P(t)]_{1,r+1} \\ &= [e^{Qt}]_{1,r+1} \\ &= \lim_{N\to\infty} \sum_{i=0}^{N} \frac{1}{i!}[(Qt)^i]_{1,r+1} \end{aligned}$$

DEFINE THE APPROXIMATION ERROR

$$e = P_f(t) - P_f^{approx.}(t)$$

THEN

$$e(t) = \lim_{N\to\infty} \sum_{i=2}^{N} \frac{1}{i!}[(Qt)^i]_{1,r+1}$$

NOTE THAT

$$|[(Qt)^i]_{1,r+1}| \le (r+1)(n\lambda t)^i$$

THEREFORE

$$\begin{aligned} |e| &\le \lim_{N\to\infty} \sum_{i=2}^{N} \frac{1}{i!}(r+1)(n\lambda t)^i \\ &\le \frac{(r+1)(n\lambda t)^2}{2} \lim_{N\to\infty} \sum_{i=0}^{N-2} (\frac{n\lambda t}{2})^i \\ &= \frac{(r+1)(n\lambda t)^2}{2 - n\lambda t}, \quad n\lambda t \ < 2 \\ &< (r+1)(n\lambda t)^2, \quad n\lambda t \ < 1 \end{aligned}$$

• SOME REMARKS

○ GOOD APPROXIMATION

$$(r+1)(n\lambda t)^2 << (1 - C_{01})n\lambda t$$

OR

$$C_{01} < 1 - n^2\lambda t$$

○ REDUNDANT SYSTEM VERSUS SIMPLE SYSTEM

$$[1 - C_{01}]n\lambda t_m < \lambda t_m$$

OR

$$C_{01} > 1 - \frac{1}{n}$$

○ IN GENERAL, $1 - C_{01}$ DECREASES AS n INCREASES

$\Rightarrow$ THERE IS AN n AT WHICH

$$\min_n (1 - C_{01})n\lambda t_m$$

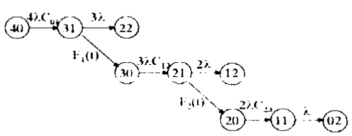
IS ACHIEVED

○ EXAMPLE

REDUNDANCY MANAGEMENT	n	C_{01}	$(1 - C_{01})n$
VOTING	4	0.992	0.032
VOTING	3	0.99	0.03
COMPARING	2	0.89	0.22

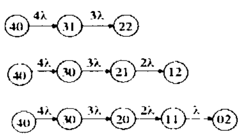
- ERROR DUE TO NEGLECTING REMOVAL TIMES

◦ OMITTED PATHS TO DEATH STATES



◦ HIGHER RATES TO DEATH STATES

— $C_{i,i+1} \leftarrow 1,\ F_i(t) \leftarrow 1$



◦ APPROXIMATION ERROR BOUND

$$
\begin{aligned}
e &= p_f - p_f^{approx.} < \sum_{j=1}^{3} \prod_{i=1}^{5-j} (5-i)(1-e^{-\lambda t})e^{-(4-i)\lambda t} \\
&\leq \sum_{j=1}^{3} \prod_{i=1}^{5-j} (5-i)\lambda = 4 \cdot 3\lambda^2 t(2 \cdot \lambda^2 t^2 + 2 \cdot \lambda t + 1) \\
&< (4\lambda t)^2, \quad (\lambda t) < \frac{1}{8}
\end{aligned}
$$

◦ GOOD APPROXIMATION

$$(1 - C_{01})4\lambda t >> (4\lambda t)^2 \Leftrightarrow C_{01} << 1 - 4\lambda t$$

- GENERAL ERROR BOUND FOR NEGLECTING REMOVAL TIMES

$$
\begin{aligned}
e &= p_f - p_f^{approx.} < \sum_{i=2}^{r} \frac{n!}{(n-i)!}(1-e^{-\lambda t})^i e^{-\frac{i}{2}(2n-i-1)\lambda t} \\
&< \sum_{2}^{r} \frac{n!}{(n-i)!}(\lambda t)^i - n(n-1)(\lambda t)^2 \sum_{i=0}^{r-2} [(n-2)\lambda t]^i \\
&= n(n-1)(\lambda t)^2 \frac{1-[(n-2)\lambda t]^{r-1}}{1-[(n-2)\lambda t} \\
&< (n\lambda t)^2, \quad n\lambda t < \frac{1}{n-2}
\end{aligned}
$$

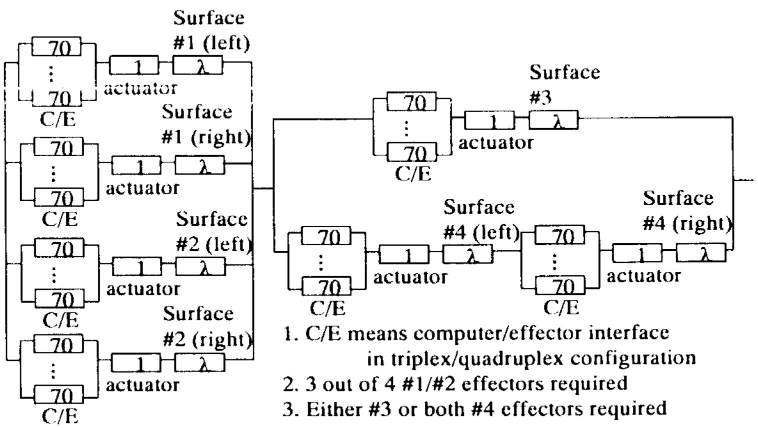
◦ GOOD APPROXIMATION

$$(1 - C_{01})n\lambda t >> (n\lambda t)^2$$

OR

$$C_{01} << 1 - n\lambda t$$

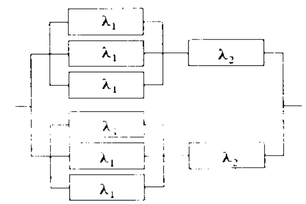
- ANALYSIS OF THE EFFECTOR BLOCK



- **SURE** AND **ASSIST** ARE NEEDED IN HIGH COVERAGE MODELS

○ A SIMPLE CASE STUDY

- EXAMPLE: DEGRADABLE 2-PLEX CONTAINING 3-PLEX–1-PLEX'S



$\lambda_1 = 10^{-5}$, $\lambda_2 = 5.0 \times 10^{-6}$, $t_m = 1.0$

$C_{01}^1 \in [0.99, 1.0]$

$C_{12}^1 \in [0.95, 1.0]$

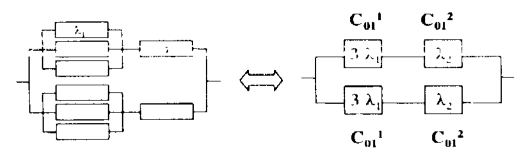
$C_{23}^1 \in [0.90, 1.0]$

$C_{01}^2 \in [0.99, 1.0]$

○ A SIMPLIFICATION WITH AN EQUIVALENT FIRST ORDER EFFECT

— $3\lambda_1$ AND λ_2 ARE OF THE SAME ORDERS OF MAGNITUDE

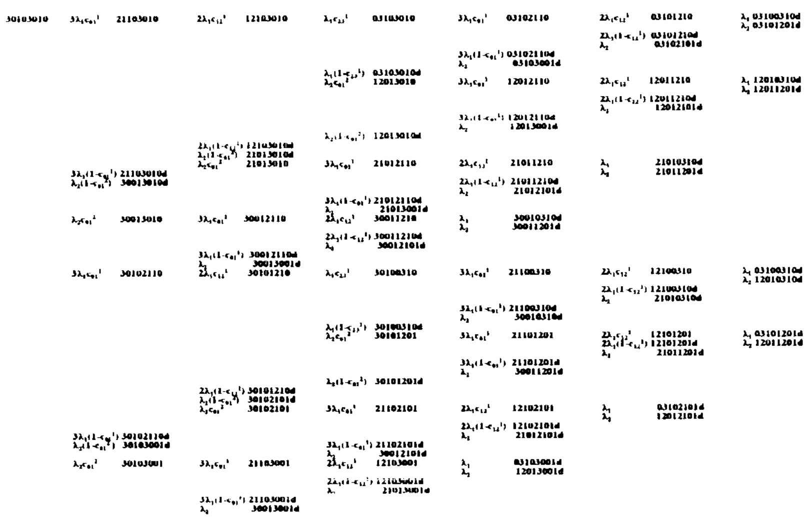
— C_{01}^1 AND C_{01}^2 ARE OF THE SAME ORDERS OF MAGNITUDE



○ SIMPLE FORMULA

$$P_f = 6\lambda_1[1 - C_{01}^1]t + 2\lambda_2[1 - C_{01}^2]t, \quad t \le t_m$$

○ STATE TRANSITION DIAGRAM



● USING **ASSIST** AND **SURE**

```
(* Markov model generation for a 2-channel 3-plex--1-plex degradable configuration*)
(* Failure rates and coverages *)
LA=1.0E-5; (* subsystem failure rate for block A (3-plex block)*)
LB=5.0E-6; (* subsystem failure rate for block B (1-plex block) *)
CA01=0.99; (* coverage for the 1st failure in block A *)
CA12=0.95; (* coverage for the 2nd failure in block A *)
CA23=0.90; (* coverage for the 3rd failure in block A *)
CB01=0.99;   (* coverage for the failure in block B *)
(* Input to SURE for coverage variation *)
"DELTA = 0.0 TO+ 1.0;" (* Delta times the coverage range = step size *)
"POINTS = 101;"
"CA01 = .99+DELTA*(1.0-0.99);" (* CA01 ranges from 0.99 to 1.0 *)
"CA12 = 0.95+DELTA*(1.0-0.95);" (* CA12 ranges from 0.95 to 1.0 *)
"CA23 = 0.90+DELTA*(1.0-0.90);" (* CA23 ranges from 0.90 to 1.0 *)
"CB01=CA01;" (* CB01 ranges from 0.99 to 1.0 *)
(* State space definition. (Array of two identical channels)*)
SPACE=(NCA: ARRAY[1..2] OF 0..3, (* NCA: Number of operative subsystems in block A *)
          NFA: ARRAY[1..2] OF 0..3, (* NFA: Number of inoperative subsystems in block A *)
          NUA: ARRAY[1..2] OF 0..1, (* NUA: Flag uncovered failures in block A when NUA=1 *)
          NCB: ARRAY[1..2] OF 0..1, (* NCB: Number of operative subsystems in block B *)
          NFB: ARRAY[1..2] OF 0..1); (* NFB: Number of inoperative subsystems in block B *)
(* Initial state definition *)
START = (2 OF 3, 2 OF 0, 2 OF 0, 2 OF 1, 2 OF 0); (* NCA[I]=3, NFA[I]=0, NUA[I]=0, NCB[I]=1, NFB[I]=0, I=0,1 *)
(* Death state definition *)
DEATHIF (NFA[1]+NFA[2]>5) (* At least one of block A or block B in each channel is inoperative *)
          OR (NFA[1]+NFB[2]>3)
          OR (NFB[1]+NFA[2]>3)
          OR (NFB[1]+NFB[2]>1)
          OR (NUA[1]+NUA[2]>=1); (* Or any uncovered failures *)
(* State transitions in channel I, I=1,2 *)
FOR I IN [1, 2];
          IF (NFB[I]=0) AND (NFA[I]=0) THEN (* 1st failure in block A *)
                    TRANTO NCA[I]=NCA[I]-1 , NFA[I]=NFA[I]+1 , NUA[I]=0 BY NCA[I]*LA*CA01; (* covered*)
                    TRANTO NCA[I]=NCA[I]-1 , NFA[I]=NFA[I]+1 , NUA[I]=1 BY NCA[I]*LA*(1-CA01); (* uncovered *)
          ENDIF;
          IF (NFB[I]=0) AND (NFA[I]=1) THEN (* 2nd failure in block A *)
                    TRANTO NCA[I]=NCA[I]-1 , NFA[I]=NFA[I]+1 , NUA[I]=0 BY NCA[I]*LA*CA12; (* covered*)
                    TRANTO NCA[I]=NCA[I]-1 , NFA[I]=NFA[I]+1 , NUA[I]=1 BY NCA[I]*LA*(1-CA12); (* uncovered *)
          ENDIF;
          IF (NFB[I]=0) AND (NFA[I]=2) THEN (* 3rd failure in block A *)
                    TRANTO NCA[I]=NCA[I]-1 , NFA[I]=NFA[I]+1 , NUA[I]=0 BY NCA[I]*LA*CA23; (* covered*)
                    TRANTO NCA[I]=NCA[I]-1 , NFA[I]=NFA[I]+1 , NUA[I]=1 BY NCA[I]*LA*(1-CA23); (* uncovered *)
          ENDIF;
          IF (NCB[I]=1) AND (NCA[I]>0) THEN (* Failure in block B *)
                    TRANTO NUA[I]=0, NCB[I]=NCB[I]-1 , NFB[I]=NFB[I]+1 BY NCB[I]*LB*CB01; (* covered*)
                    TRANTO NUA[I]=1, NCB[I]=NCB[I]-1 , NFB[I]=NFB[I]+1 BY NCB[I]*LB*(1-CB01); (* uncovered *)
          ENDIF;
ENDFOR;
```

○ FINITE REMOVAL TIMES CAN BE EASILY INCORPORATED

○ ANALYTIC MODEL WITH MINIMAL STATE DIMENSION

$$\dot{P}(t) = P(t)Q(t), \quad P(0) = I$$

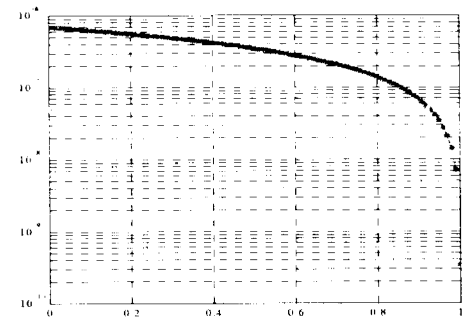
AND Q IS GIVEN BY

$$\begin{bmatrix}
-6\lambda_1 - 2\lambda_2 & 6\lambda_1 C^1_{01} + 2\lambda_2 C^2_{01} & 0 & 0 & 0 & 0 & 6\lambda_1[1 - C^1_{01}] + 2\lambda_2[1 - C^2_{01}] \\
0 & -10\lambda_1 - 4\lambda_2 & 4\lambda_1 C^1_{12} + 6\lambda_1 C^1_{01} + 2\lambda_2 C^2_{01} & 0 & 0 & 0 & 4\lambda_1[1 - C^1_{12}] + 6\lambda_1[1 - C^1_{01}] + 2\lambda_2[1 - C^2_{01}] + 2\lambda_2 \\
0 & 0 & -12\lambda_1 - 6\lambda_2 & 2\lambda_1 C^1_{23} + 4\lambda_1 C^1_{12} + 6\lambda_1 C^1_{01} + 2\lambda_2 C^2_{01} & 0 & 0 & 2\lambda_1[1 - C^1_{23}] + 2\lambda_2[1 - C^2_{10}] + 6\lambda_1[1 - C^1_{01}] + 4\lambda_1[1 - C^1_{12}] + 4\lambda_2 \\
0 & 0 & 0 & -18\lambda_1 - 8\lambda_2 & 12\lambda_1 C^1_{01} + 4\lambda_1 C^1_{12} & 0 & 12\lambda_1[1 - C^1_{01}] + 4\lambda_1[1 - C^1_{12}] + 2\lambda_1 + 8\lambda_2 \\
0 & 0 & 0 & 0 & -10\lambda_1 - 6\lambda_2 & 8\lambda_1 C^1_{12} & 8\lambda_1[1 - C^1_{12}] + 2\lambda_1 + 6\lambda_2 \\
0 & 0 & 0 & 0 & 0 & -4\lambda_1 - 4\lambda_2 & 4\lambda_1 + 4\lambda_2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

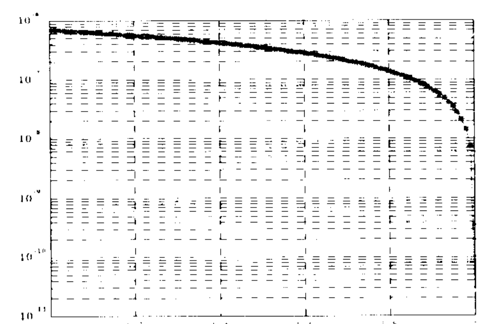
○ THE ABOVE RESULTS IN THE SAME SIMPLE FORMULA

$$P_f = [P(t)]_{(1,7)} \approx [Q]_{(1,7)}t = 6\lambda_1[1 - C^1_{01}]t + 2\lambda_2[1 - C^2_{01}]t, \quad t \le t_m$$

○ EFFECT OF SIMPLIFICATION



○ MATRIX EXPONENTIAL V.S. **ASSIST/SURE**



- KEY TO ENHANCED RELIABILITY—HIGH COVERAGE

○ CURRENTLY ACHIEVABLE VALUE IN FTFCS?

— $1 - C_{01} \approx 10^{-1}$

○ IMPROVEMENT DESIRABLE?

—REDUCTION OF $1 - C_{01}$ BY SEVERAL ORDERS OF MAGNITUDE

○ ADEQUATE VALUE?

—$1 - C_{01} \approx n^2 \lambda t_m$

○ WHEN THE ABOVE IS ACHIEVED

—**SURE** IS NEEDED FOR ACCURACY

—**ASSIST** IS NEEDED FOR MODELING

○ A BY-PRODUCT OF **ASSIST**

—TRANSITION RATE MATRIX OF A MARKOV PROCESS

References

[1] Bavuso, Dugan, Trivedi, Rothmann, and Smith, Analysis of typical fault-tolerant architectures using HARP, *IEEE Trans. on Reliability*, vol.R-36, pp 176-185, 1987.

[2] R.W.Butler, An abstract language for specifying Markov reliability models, *IEEE Trans. on Reliability*, vol.R-35, pp 595-601, 1986.

[3] R.W.Butler, and A.L.White, SURE reliability analysis: program and mathematics, *NASA Technical Paper 2764*, 1988.

[4] R.W.Butler, The SURE approach to reliability analysis, *IEEE Trans. Reliability*,vol.41, pp 210-218, 1992.

[5] Dugan, and Trivedi, Coverage modeling for dependability analysis of fault tolerant systems, *IEEE Trans. Computers*, vol.38, pp 775-787, 1989.

[6] General Electric Company, *Self-Repairing Digital Flight Control System Study*, Report# AFWAL-TR-88-3007, 1987.

[7] S.T.Trivedi, *Probability & Statistics with Reliability, Queuing, and Computer Science Applications*, Chapter 6, Prentice Hall, 1982.

[8] A.L. White, Reliability estimation for reconfigurable systems with fast recovery, *Microelectronics Reliability*, vol.26, pp 1111-1120, 1986.

[9] Dugan, Trivedi, Smotherman, and Geist, The hybrid automated reliability predictor, *J. Guidance*, vol.9, pp.319-331, 1986.

[10] N.E.Wu, Hardware reduction through use of control surface redundancy, *Technical report to General Electric Company*, 1991.

[11] D.L.Isaacson, and R.M.Madsen, *Markov Chains Theory and Applications*, John Wiley & Sons, 1976.